Preliminary Program Agenda as of February 12, 2013

Software Assurance (SwA) Spring Forum 2013

Theme: Software Supply Chain Risk Management (Sw-SCRM)

5-7 March, 2013 at

National Institute of Standards and Technology (NIST),

100 Bureau Drive, Gaithersburg, MD 20899

	5 March (Tuesday)	6 March (Wednesday)	7 March (Thursday)
9:00 AM	**Opening –** Joe Jarzombek, DHS **Welcome speaker – Charles Romine, Director, ITL, NIST** **FISMA Enabled SCRM** Ron Ross, NIST	**Opening –** Joe Jarzombek, DHS **Keynote speaker – Edna Conway, CISCO** **Panel on ICT Supply Chain Exploitation** Kevin Dillon, DHS Ken Crowther, MITRE Jon Boyens, NIST	**Opening –** Joe Jarzombek, DHS **Keynote speaker – Roberta "Bobbie" Stempfley, Acting Assistant Secretary, Cybersecurity and Communications, DHS** **Securing the Supply Chain** Marcus Sachs, Verizon
	10:30 AM Break	***10:30 AM Break***	***10:30 AM Break***
11 AM	**We Can't Blindly Reap the Benefits of a Globalized ICT Supply Chain** Don Davidson, DoD Jon Boyens, NIST Dr. Sandor Boyson, UMD	**How International Standards Efforts Help Address Challenges in Today's Global Market Place** Michele Moss , Booz Allen Hamilton Nadya Bartol, UTC Jed Pickel, Microsoft Eric Winterton, Booz Allen Hamilton (invited) Andras Szakal, The Open Group	**Ensuring Your Development Processes Meet Today's Cyber Challenge** Michele Moss , Booz Allen Hamilton Mary Beth Chrissis, SEI Andy Murren, D&T Vehbi Tasar, (ISC)^2
	12:30 Lunch	***12:30 Lunch***	***12:30 Lunch***
1:30PM	**SCRM Perspective on 3rd Party Software Assessment** Marc Jones, CAST Devon Bryan, ADP Jeff Voas, NIST – Mobile Apps Kevin Greene, DHS S&T	**International Perspectives on SCRM** Ian Bryant, TSI, UK **Software ID Tags Support SCRM** Steve Klos, TagVault John Richardson, Symantec Doug White, NIST	**Scaling SwA -- Beyond Static and Dynamic Analysis with Contrast** Jeff Williams, AspectSecurity **Managing Risk in the Software Supply Chain through Software Code Governance** Andrew Chou , Coverity
	3:00 PM Break	***3:00 PM Break***	***3:00 PM Break***
3:30PM	**Advancing SCRM with Standardized Inspection Technology** Roger Stewart, Stewart-Priven Group **Testing Panel** John Keane, DoD Ken Hong Fong, IDA **Static Analysis Tool Exposition (SATE)** Paul Black, NIST	**Building a Body of Knowledge for ICT Supply Chain Risk Management"** Dan Shoemaker, UD-M **Education Panel** Dennis Phelan, SRA Peggy Maxson, DHS Andy Caulfield, NSA	**Open Source and the Software Supply Chain: A Look at Risks vs. Rewards** Wayne Jackson, Sonatype **Open Source SCRM Panel** David Wheeler, IDA Dan Risacher, DoD Jeff Williams, AspectSecurity Wayne Jackson, Sonatype Luke Berndt, DHS S&T (invited)
	5:00 PM Wrap-Up	***5:00 PM Wrap-Up***	***5:00 PM Wrap-Up***

Our theme is Software Supply Chain Risk Management (Sw-SCRM)

Regardless of intent, software can become tainted by malware, exploitable weaknesses and vulnerabilities. Whether software becomes compromised by ignorance, negligence, or malfeasance, the end result of tainted products can be dire for those who inherit the residual risk exposure. Just as with food and pharmaceuticals, software can be corrupted in ways that put users, organizations, and missions at risk. Thus each participant in the supply chain requires an appreciation of controls and processes that should be in the potential paths software can take before it is acquired and put into use. The presenters at the March 2013 SwA Forum will explore progress, research, and challenges in addressing Sw-SCRM.

See https://buildsecurityin.us-cert.gov/bsi/events/1417-BSI.html for the latest agenda and logistical information. Although the cost is FREE, **you must register for the Forum by COB 25 February 2012** in order to enter the NIST campus. SwA Forum staff will not be at NIST gates to provide entry for non-registered individuals.

We Can't Blindly Reap the Benefits of a Globalized ICT Supply Chain!

Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) seeks to manage and mitigate cyber and supply chain risk throughout an acquisition and sustainment lifecycle for an element or a system. It is a multi-disciplinary challenge which requires contributions and collaboration among many disciplines. Key areas include systems engineering, system security engineering, information security, software development, application security, supply chain and logistics planning and management, IT resiliency, and risk management. While many areas are making great strides in developing and implementing best practices and tools to combat their individual cyber challenges, it is imperative for successful enterprise risk management to view the challenge holistically and align common best practices and initiatives, some from/for the public sector and some from/for the private sector.

SCRM Perspective on 3rd Party Software Assessment

How do we ensure that the right levels of due diligence are being applied to help assure the confidentiality, integrity, and availability of the sensitive information ADP entrusts to our third party vendors in our supply chain? Do we need an approach like that for FedRAMP that uses a "do once, use many times" framework that saves cost, time, and staff required to conduct redundant agency security assessments? What would such a standardized software supply chain approach consist of for assessment, authorization, risk management, and continuous monitoring for software products and services.

Advancing SCRM with Standardized Inspection Technology

Technology exists today that can make a huge improvement minimizing risk along the supply chains and improve delivery of secure-high quality products, on-time and within budget. And no changes to standards, legislation or acquisition models are needed. Accepting this approach to Supply Chain Risk Management (SCRM) by industry and government means adopting policies to:

- Impose contract stipulations on the prime contractor, such as common tools and process use, that must also apply to all vendors along their supply chain, and their vendor's supply chains,
- Require a common, standardized platform of: tools, process and training along the supply chains for consistently performing ongoing product risk assessments through defect identification and removal on pre-code product definition artifacts (e.g., contracts, requirements, architecture, design, interfaces), where past studies report 70+% of product defects historically originate,
- Require results of each product risk assessment be made available to both the prime contractor and the government program manager in the form of an automated, tool-generated report with common format and content,
- Include contract leverage for the government program office based upon their ongoing evaluations of the resulting product risk visibility,
- Use a tool-enabled, standard-compliant Inspection process for defect identification and removal in Product Definition artifacts along the supply chain and for achieving the ongoing risk assessments and reports.

How International Standard Efforts Help Address Challenges in Today's Global Marketplace

An increasingly distributed and global information and communication technology (ICT) supply chain brings challenges to US Government and industry. Identifying and mitigating risks involves looking beyond

your organization and understanding and managing risks caused by the lack of visibility in the ICT supply chain. Recent research indicates that current ICT supply chain risk management practices tend to have a tactical focus motivated primarily by compliance rather than a strategic integrated approach. However, there are a number of existing international standards and several under development that when used in combination will help this problem. Using these standards together will provide security assurance process for information security governance, software development, Supply Chain Risk Management (SCRM) and should result in reducing ICT supply chain risk.

International Perspectives on SCRM

In response to the 2010 UK National Security Strategy, which identified Cybersecurity as one of the four "Tier One" risks of particular concern, the UK has recently formed a public-private platform for enhancing the overall software and systems culture, with the objective that all software should become designed, implemented and maintained in a secure, dependable and resilient manner. This presentation explains the goals and structure of the new UK Trustworthy Software Initiative (TSI) and its perspective on software supply chain risk management (SCRM).

Software ID Tags Support Supply Chain Risk Management (SCRM)

Would you fly on an airline that did not verify passenger identities, or that let unknown or high risk passengers on a flight? How about an airline that was unable to scan baggage for known threats, or be able to trace each bag back to its owner? This is, unfortunately, the position that IT organizations are placed into every day. Software application installers install hundreds to thousands of files on a system with no way of:

- validating that only authorized software is installed
- associating installed files with a specific application and version
- reporting that any of an applications files have modified
- identifying if installed applications have known vulnerabilities

Building a Body of Knowledge for ICT Supply Chain Risk Management

The speakers in this session will propose a set of supply chain risk management (SCRM) activities and practices for information and communication technologies (ICT). This set can be used as a starting point to create a body of knowledge in SCRM to ensure the integrity of ICT products.

Ensuring Your Development Processes Meet Today's Cyber Challenges

While security in the physical world can be addressed using controls such as guns, gates, and guards, the virtual world requires other mechanisms to ensure the confidentiality, availability, and integrity of products and services. Much of what today's products, services, infrastructures, and institutions do is automated by software, thereby increasing our dependence on how safety and security are addressed in the virtual world. As software continues to evolve and we find new ways to leverage the virtual world in our day–to-day activities, the volume and our reliance on software grows exponentially. Therefore, it is increasingly important to have confidence that products operate as intended and only as intended to ensure the resilience and reliability of the functions they support. Much of software is acquired forcing consideration of these critical qualities into the supply chain. Achieving such confidence ultimately relies on good system and software engineering knowledge, processes, and technology. Fortunately, many resources are

available. This article provides a brief survey of some of these resources, such as process capability frameworks, secure lifecycle practices, and implementation approaches.

Scaling SwA -- Beyond Static and Dynamic Analysis with Contrast

Automation is the only way to secure an entire application portfolio -- but today's website and code scanning tools take forever and make too many mistakes – worst of all, they require experts, so they don't scale. Fortunately, the "big data" revolution has pointed the way to a better approach. We can instrument running applications with passive security sensors, and gather huge amounts of data from inside running apps. This approach correlates static, dynamic, and runtime data views of an application together in realtime. Jeff will show how analyzing this data leads to significantly more coverage and better accuracy than existing tools. We'll also discuss how this new approach to application security scales easily and integrates naturally with the way modern software development projects actually work.

Managing Risk in the Software Supply Chain through Software Code Governance

With the increasing complexity of software applications, shrinking IT budgets and the spiraling cost of developing software, many organizations in both the public and private sectors are turning to third-party software suppliers including outsourced teams, partners and open source to develop their applications. According to a recent study1 conducted by Forrester Consulting and Coverity, almost all organizations are using some form of third-party code in their products, and over forty percent rely on software from three to five different software suppliers.

Open Source and the Software Supply Chain: A Look at Risks vs. Rewards

For most of its history, software has been written – applications consisted primarily of custom developed code and internally developed components with only a small fraction of code sourced from outside the organization. Development efforts followed a "waterfall" methodology and projects spanned months or even years. The widespread use of cloud-based infrastructures and the rise of open-source technologies during the past decade have heavily influenced the software development landscape with start-ups and established organizations demanding increased flexibility and improved time to value in the way software is developed and delivered. As a result, modern software development and the resulting software supply chain have become increasingly component-based, where applications are assembled from existing components rather than written from scratch. Enterprise applications today are typically built using 75-80 percent open source components1, with custom code comprising the rest. So, what does today's software development landscape look like at what are the risks to the software supply chain?